ClearPath Enterprise Servers

Authentication Sentinel for OS 2200
User Guide

UNISYS

© 2004 Unisys Corporation.
All rights reserved.

ClearPath OS 2200 Release 8.2

September 2004

Printed in USA
4729 2016–000

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product or related information described herein is only furnished pursuant and subject to the terms and conditions of a duly executed agreement to purchase or lease equipment or to license software. The only warranties made by Unisys, if any, with respect to the products described in this document are set forth in such agreement. Unisys cannot accept any financial or other responsibility that may be the result of your use of the information in this document or software material, including direct, special, or consequential damages.

You should be very careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used.

The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Notice to U.S. Government End Users: This is commercial computer software or hardware documentation developed at private expense. Use, reproduction, or disclosure by the Government is subject to the terms of Unisys standard commercial license for the products, and where applicable, the restricted/limited rights provisions of the contract data rights clauses.

Correspondence regarding this publication can be e-mailed to **doc@unisys.com**.

Unisys and ClearPath are registered trademarks of Unisys Corporation in the United States and other countries.
All other brands and products referenced in this document are acknowledged to be the trademarks or registered trademarks of their respective holders.

ClearPath Enterprise Servers

Authentication Sentinel for OS 2200

User Guide

ClearPath OS 2200 Release 8.2

4729 2016–000

ClearPath Enterprise Servers

Authentication Sentinel for OS 2200

User Guide

ClearPath OS 2200 Release 8.2

4729 2016–000

Bend here, peel upwards and apply to spine.

Contents

Section 1. Introduction

1.1. Authentication Sentinel Components 1–1
1.2. About This Guide 1–2
1.2.1. Purpose 1–2
1.2.2. Audience 1–2
1.2.3. Notation Conventions 1–2

Section 2. Installation

2.1. Installing the Slot Appliances 2–1
2.2. Software Requirements 2–2
2.3. Software Installation 2–3

Section 3. Configuration and Setup

3.1. Configure COMAPI and User Authentication 3–1
3.2. Install and Configure 2200 Network Authentication using Security Client 3–2
3.3. Set Up User Accounts 3–3
3.4. Set Up User Workstations 3–3
3.5. Verify Network Authentication 3–4

Section 4. Monitoring and Troubleshooting

4.1. AuthCheck Monitor Program 4–1
4.2. Run-Time Diagnostics 4–2
4.2.1. Sign-On Error Messages 4–2
4.2.2. Console Messages 4–2
4.2.3. Web Transaction Server Network Authentication Errors 4–2
4.3. Troubleshooting Methods 4–3
4.4. Hardware Troubleshooting 4–4

Appendix A. TIP/Demand Examples

Appendix B. Related Documents

Figures

2–1. Installing a Slot Appliance 2–2

4–1. Location of Hard Reset Button 4–4

Section 1
Introduction

Authentication Sentinel consists of both hardware and software components that provide 2200 Network Authentication in a security environment without the need for general Windows servers and the configuration and management tasks they require.

Network Authentication for OS 2200 allows OS 2200 users to be authenticated for access to an OS 2200 server using their Windows credentials (username and password) without being resolicited for those credentials.

OS 2200 access paths that can use network authentication include

- 2200 TIP/demand.
- Web Transaction Server for ClearPath OS 2200 (formerly WebTS). Web Transaction Server can use network authentication for access protection of transactions and page files.
- Network Authentication APIs: AUTH_USER & AUTH_CONTEXT. These APIs allow non-TIP or demand applications and middleware to authenticate with network credentials without starting an OS 2200 communication session.

1.1. Authentication Sentinel Components

Authentication Sentinel components include

- Redundant slot appliances with preloaded software; installed in a PCI rack
- OS 2200 Security Administrator software
- Messaging Integration Services (NTSI) software
- User Authentication software
- Other software required to support the above

A slot appliance is a single-board computer (SBC) with flash storage. OS 2200 Security Administrator and Messaging Integration Services are OS 2200 products that support OS 2200 security functions.

OS 2200 Security Administrator lets you configure user-id/passwords as well as create privileges for OS 2200 users. It is also used to install and configure network authentication for each OS 2200.

Messaging Integration Services provides Kerberos, Windows NT LAN Manager (NTLM), and Network User-id/password authentication as alternatives to local OS 2200 security authentication. Authentication Modules (AMs) link with the User Authentication (FLEX) product. Single sign-on is achieved when Kerberos or NTLM are used. User-id/password requires users to enter their Windows domain username and password when solicited.

1.2. About This Guide

This section provides information about the purpose and audience for the information in this guide, and notations used in the guide.

1.2.1. Purpose

This guide describes Authentication Sentinel for OS 2200 installation, configuration, and setup. To use this guide, you should understand the OS 2200 Exec operating system and installation procedures for software products. To install the hardware, you should be an experienced Unisys customer engineer.

This guide contains all the information available at the time of publication. Technical changes that were not available at that time are supplied in PLE 18106493. To obtain copies of the PLE, contact your Unisys representative.

1.2.2. Audience

This guide is for site administrators and other technical personnel who are responsible for the Authentication Sentinel for OS 2200 and 2200 Network Authentication environment.

1.2.3. Notation Conventions

Format statements in the guide follow these conventions for syntax:

- The pound symbol (#) represents the word "number." The italicized expression *file#* means "file number"; the italicized word *file*, if it is not immediately followed by #, means "file name."
- Italicized text represents data that you supply; this is shown in lowercase letters, although you can enter the actual data in either uppercase or lowercase letters.
- Uppercase, nonitalicized text shown in format statements represents something that you must enter exactly as shown, although you can use either uppercase or lowercase letters.
- Brackets surround text that is optional:

  ```
  COPY[,options]
  ```

- Brackets, braces, and vertical lines are not part of the command syntax; do not type them.
- A semicolon (;) is the OS 2200 continuation character, which you must use if a single command or data image extends beyond one line. In input format statements in this

manual, semicolons are used simply to split long lines for display purposes; you do not need to type them in as shown unless you want to split your input lines at those points.

Section 2
Installation

Installation of Authentication Sentinel for OS 2200 requires installing redundant slot appliances into an expansion rack and installing software components on both the OS 2200 and a Windows workstation.

2.1. Installing the Slot Appliances

Authentication Sentinel for OS 2200 consists of two slot appliances to allow for redundant security. Installation should be performed only by a qualified Unisys customer engineer.

Note: *For increased resiliency, each slot appliance should be located on a different PCI rack and power domain.*

To install the slot appliances, proceed as follows:

1. Make sure the expansion rack is powered off.
2. Insert a slot appliance into an available PCI slot on the expansion rack.
3. Connect the private Ethernet cable into the upper RJ45 connector of the slot appliance (Figure 2–1). The private Ethernet port is the port that connects the slot appliance to the private HMP LAN. The private Ethernet port has a static IP address of either 192.168.57.101 for Type 1 slot appliances or 192.168.57.102 for Type 2 slot appliances. To identify the type of slot appliance, look for a label on the slot appliance that has a 16-character identifier starting with the word "Unisys," for example, UnisysA0C05BAA11. The letter immediately after the word "Unisys" indicates the type of slot appliance: A (Type 1), B (Type 2), or C (None).
4. Connect the public Ethernet cable into the middle RJ45 connector of the slot appliance (Figure 2–1). The public Ethernet port is the port that connects to the customer's LAN. The public Ethernet port on the slot appliance is configured to use DHCP. Therefore, the customer's LAN must have a DHCP server that will dynamically give the slot appliance an IP address for its public Ethernet port.
5. Power on the PCI rack.
6. Repeat steps 1 through 5 for the second slot appliance.

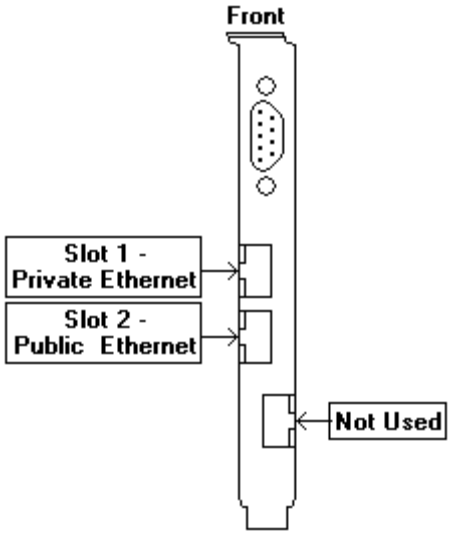

Figure 2–1. Installing a Slot Appliance

2.2. Software Requirements

The following Unisys products must be installed to run OS 2200 Network Authentication.

- Communications Platform (CP)
- Communications Application Program Interface (COMAPI) must be installed on the OS 2200 server. Mode A must be used.
- User Authentication (FLEX) must be installed on the OS 2200 server.
- The OS 2200 component of Messaging Integration Services (NTSI) must be installed on the OS 2200 server. Mode A must be used.
- The Security Administration Agent must be installed on the OS 2200 server and the Client must be installed on a workstation accessible to the 2200 Security Administrator.
- Each workstation that requires OS 2200 access must have a Uniscope emulator installed and configured. For single sign-on, the emulator must support the enhanced TIP and demand protocol for obtaining and passing tickets. Check with your emulator vendor.

Note: *You must install and use Mode A of COMAPI and Mode A of Messaging Integration Services with Authentication Sentinel for OS 2200. If you already have a Messaging Integration Services Mode A installed on OS 2200 and it is not used for network authentication, you must move that application to another mode of Messaging Integration Services. See the* Messaging Integration Services Help *for details on how to install and use other modes. If your Mode A is already being used for network authentication, then Authentication Sentinel for OS 2200 replaces your Windows servers.*

2.3. Software Installation

Refer to the *Software Products Installation Guide* for information on installing the software products required for Authentication Sentinel for OS 2200. The following table lists the primary reference document for each product.

Product	Reference Document
Communications Platform (CP)	*Communications Platform Configuration and Operations Guide*
Communications Application Program Interface (COMAPI)	*Communications Application Program Interface User's Guide*
User Authentication (FLEX)	*Flexible User Authentication Administration Guide*
Messaging Integration Services (NTSI) – OS 2200 component	*'Installing the Software Components on the 2200 Servers' in Messaging Integration Servers for ClearPath OS 2200 Help*
Security Administration Agent (OS 2200) and Client (workstation)	*Security Administration for ClearPath OS 2200 Help*

Section 3
Configuration and Setup

Following are the configuration requirements for 2200 Network Authentication. Some configuration steps have been done for you, but some remain under your control because they involve site-specific attributes, such as your Windows domain name.

3.1. Configure COMAPI and User Authentication

1. See the *COMAPI User's Guide* to configure COMAPI.
2. After configuring COMAPI, start the COMAPI background run.
3. Refer to the *Flexible User Authentication Administration Guide* to create the necessary OS 2200 user accounts and ACRs for user authentication.
4. Run the Messaging Integration Services configurator on the OS 2200 server. The sample Authentication Sentinel for OS 2200 configuration is in

   ```
   SYS$LIB$*NTSI-SAMPLES.PARMS/CITADEL
   ```

   Enter the following:

   ```
   @SYS$LIB$*NTSI.CONFIGURATOR  SYS$LIB$*NTSI-SAMPLES.PARMS/CITADEL
   ```

   You must modify this Authentication Sentinel for OS 2200 sample configuration element before running the Messaging Integration Services configurator to make sure the IP address of your 2200 is on the TTH-IP-ADDRESS statement.

5. The Network Authentication Modules (AMs) must be copied into the 2200 User Authentication subsystem to support Network Authentication for TIP and demand sessions. Perform these copies before relinking and starting the ASIS background run.

   ```
   @COPY,A SYS$LIB$*NTSI-SAMPLES.AM02$OM,SYS$LIB$*ASIS-OMS.

   @COPY,A SYS$LIB$*NTSI-SAMPLES.AM03$OM,SYS$LIB$*ASIS-OMS.

   @COPY,A SYS$LIB$*NTSI-SAMPLES.AM07$OM,SYS$LIB$*ASIS-OMS.
   ```

6. Start ASIS — the User Authentication background run — using the relink option.

Note: *Make sure both the COMAPI and the ASIS background runs come up automatically after an OS 2200 system reboot. After these runs come up, the Messaging Integration Services configurator must also be rerun. Locate these calls in a runstream that starts on every system reboot.*

3.2. Install and Configure 2200 Network Authentication using Security Client

You use Security Client to perform the following operations to install and configure 2200 Network Authentication.

- Join the Authentication Sentinel for OS 2200 slot appliances to your Windows domain.
- Create an OS 2200 computer account in your Windows domain.
- Configure specific 2200 Network Authentication attributes.

Refer to the *Security Administration for ClearPath OS 2200 Help,* which is part of Security Client, for specific information.

Once 2200 Network Authentication is installed, Security Client lets you view the current network authentication information as well as update and delete network authentication.

Note: *When you start Security Client, you are required to sign onto a specific OS 2200 using a local OS 2200 account and password. It is for this specific OS 2200 that you are installing network authentication, and your account must have the appropriate administration rights before you can install network authentication.*

2200 Network Authentication commands in Security Client include:

- Delete Network Authentication.

  Used to clear all current network authentication settings.
- Delete Network SPN

  Used to delete service principal names (SPNs) if necessary.
- Display Network Authentication

  Used to view the current network authentication configuration. Helpful for diagnosing problems.
- Install Network Authentication

  Used to install and configure network authentication on the OS 2200.
- Install Network SPN

  Used to install service principal names (SPNs).
- Update Network Authentication

  Used to update the current configuration of network authentication on the OS 2200.

Notes:

- *The network authentication configuration is kept in a file on OS 2200 named NETWORK$*CONFIG$. This file is cataloged as public and exclusively assigned to the Messaging Integration Services (NTSI) subsystem so it is automatically accessible by the Security Client Agent, the Messaging Integration Services subsystem, and the Authentication Modules (AMs). Make sure this file is secured and never rolled out. If you put access controls (ACRs) on this file, make sure all these entities have read and write access rights.*

- *When Security Client is used to configure network authentication, you are asked for a Windows domain\username and password. You must know exactly what kind of account is needed and what rights the account needs before issuing the Security Client command.*

3.3. Set Up User Accounts

If they do not already exist, follow this procedure to set up user accounts:

1. Create user accounts in your Windows security domain; one for each OS 2200 user. If you plan on using exact match to map the network user to the local 2200 user-id, the network account name must match the OS 2200 user-id. Normally, you do not use exact match.
2. Use Security Client to create local OS 2200 user-id accounts to be associated with the network user accounts. If the authentication type you are using for a user-id is user-id/password, then the Authentication Type option must be set to 7. Otherwise, it can be left blank.
3. Insert the user's full Windows network name into the Network User-id box in each OS 2200 user-id record. This step is required if you configured Network-Id Match for mapping the network user to an OS 2200 local user.

   Note: *The network user-id must be entered in all uppercase characters.*

   For example, to map network username *JohnsonRA* in domain *MyCompany.com* to the OS 2200 user-id *john,* type MYCOMPANY.COM\JOHNSONRA in the Network User-id box of the john1 user-id record.

   Note: *If you want to inhibit local sign-on to the OS 2200 by this user-id, select the Authentication only via Network User-id box in the Security Client Access menu or do not supply a local OS 2200 password. Some users may still need to sign on to the OS 2200 Demand locally for administration work or to use other OS 2200 products that require a local password.*

3.4. Set Up User Workstations

Follow this procedure to use Kerberos or NTLM for single sign-on.

1. Install and configure a UNISCOPE emulator that supports the enhanced TIP and demand protocol for passing tickets. The INFOConnect 2001 v5.0 Accessory Manager and KMSystem's eXpress Plus support this authentication protocol. Other UTS emulators may also support this authentication protocol. Check with your vendor.
2. For each emulator, configure a path for NTLM or Kerberos authentication using the emulator's configuration tool.
3. For Kerberos authentication, you must supply the OS 2200 computer account as the target.

3.5. Verify Network Authentication

After you have completed configuration, verify 2200 Network Authentication as follows.

1. From your Windows workstation, sign on to the OS 2200 server using:

   $$OPEN <*path*>

   If you are using Kerberos or NTLM Authentication, you should not be asked to supply the OS 2200 user-id or password.

   If you are using 2200 Windows User-Id Authentication, you may be required to supply a domain name in front of your username/password. For example:

   domainname\username/password

2. Use Web Transaction Server to access a Kerberos or NTLM-protected transaction or page file.
3. Use the AUTH_API or AUTH_CONTEXT APIs for network authentication.

Section 4
Monitoring and Troubleshooting

Because the Authentication Sentinel slot appliances do not accommodate a keyboard, monitor, or mouse, no local or remote administration or monitoring of the slot appliance can be done other than outlined below. This includes access and use of Message Integration Services local administration and Windows tools (for example, Event Viewer).

4.1. AuthCheck Monitor Program

The AuthCheck program monitors the state of the Authentication Sentinel slot applicane and informs you through console messages or printout if there are problems. It can also attempt to automatically recover the network authentication configuration on the Authentication Sentinel for OS 2200 nodes if they become out-of-sync with the network configuration on the OS 2200.

It is critical that the AuthCheck program be started automatically after each OS 2200 reboot or run periodically during the day. Running with the A and Z options is recommended.

To start AuthCheck, enter the following:

```
@SYS$LIB$*NTSI-SAMPLES.AUTHCHECK, <options>
```

Options	Description
None	The program runs once and displays results with printouts.
A	When the Z option is set, the program sends a console message when only one node is configured with Messaging Integration Services. When the Z option is set without the A option, no console message is sent when this situation is detected. Running with the A option is recommended.
D	Debug option, extra prints are produced. Normally, you will not run with the D option.
R	The program attempts to recover from the error situation. This means reinserting the current 2200 network authentication configuration onto the nodes. If network authentication cannot be recovered, the program terminates even if the Z option is set.
Z	The program runs as a background run. It sends console messages when errors are encountered. If network authentication enters an unknown state, the program terminates. Running with the Z option is recommended. ***Note:*** *You may not want to start AuthCheck with the Z option set initially until Network Authentication is installed and working. This avoids console messages when Network Authentication is not installed yet or is in the process of being installed.*

4.2. Run-Time Diagnostics

The following sections provide information about run-time diagnostics for

- Sign-on error messages
- Console messages
- WebTransaction Server network authentication errors

4.2.1. Sign-On Error Messages

If you attempt to sign-on to TIP or demand, some authentication failure messages are displayed on the screen. If a message is displayed, use it to help determine the problem. If no message is displayed and you think the authentication should have succeeded, you need to investigate further using other methods and tools.

4.2.2. Console Messages

If there is a problem with the Authentication Sentinel that makes signon to TIP or demand unavailable, console messages are sent to inform the operator. These console messages are sent at progressively longer intervals so as not to flood the console. Use these unsolicited console messages to help diagnose problems. The message sent includes the name of the authentication module that detected the problem.

AM02$OM is the AM that handles Kerberos authentications

AM03$OM is the AM that handles Windows NT LAN Manager (NTLM) authentications

AM07$OM is the AM that handles Userid/Password authentications

When the User Authentication (FLEX) product detects an error or an abnormal situation during sign-on to TIP or demand, it may also send a console message. Use these messages to monitor problems and issues as they appear.

If the AuthCheck program is running as a background run, it sends console messages when errors or abnormal situations are detected. This includes the situation where network authentication is still working but one of the two Authentication Sentinel for OS 2200 servers is not. AuthCheck can be executed with the R option to attempt automatic recovery of the Authentication Sentinel for OS 2200 servers. If this fails or the R option is not used, manual recovery is required using Security Client to reinstall the network authentication configuration.

4.2.3. Web Transaction Server Network Authentication Errors

If a Web page or transaction is configured for network authentication protection and the user cannot be authenticated with his or her network credentials, then the browser opens a window that solicits an OS 2200 user-id and password. If this window is displayed and you don't think it should have been displayed, it may indicate a problem with network authentication. See the *Web Transaction Server Administration Guide* for more details on Web Transaction Server diagnostics.

4.3. Troubleshooting Methods

For further troubleshooting information or more details, see the troubleshooting procedures in *Messaging Integration Servers for ClearPath OS 2200 Help* and *Security Administration for ClearPath OS 2200 Help*.

The following methods of troubleshooting Authentication Sentinel for OS 2200 may be helpful:

- Run the AuthCheck program without any options to see what is displayed. Enter

  ```
  @SYS$LIB$*NTSI-SAMPLES.AUTHCHECK
  ```

  If the AuthCheck program is also running as a background run, check for any console messages it might have sent. If it was running but has terminated, check its print file for any pertinent information.

- Run the Messaging Integration Services (NTSI) configurator with the D option. Enter

  ```
  @SYS$LIB$*NTSI.CONFIGURATOR,D
  ```

  This displays the current Messaging Integration Services configuration. If the configurator has not been rerun since the NTSI subsystem has been deactivated (system reboot or a new NTSI install), the display information shows zeros. If it shows that nothing is configured, rerun it and apply the following Authentication Sentinel for OS 2200 configuration:

  ```
  @SYS$LIB$*NTSI.CONFIGURATOR  SYS$LIB$*NTSI-SAMPLES.PARMS/CITADEL
  ```

  Note: *Apply the configuration qual*file.ele you have set up. It may not be this qual*file.ele.*

- Run Security Client from a workstation and select Display Network Authentication from the Display menu. Check the state of each Authentication Sentinel for OS 2200 server and the configuration values for this OS 2200. If there is a problem or error, reinstall or update the configuration information.

- For User Authentication (FLEX) traces, turn on the FLEX traces via the ASIS utility and study the results. The ASIS utility (@ASISUT) is used to administer FLEX. The TYPES command lists the current registered AMs. You should have four on your OS 2200 system: AM0 (traditional), AM02 (Kerberos), AM03 (NTLM), and AM07 (User-id/Password).

  Use the BRKPT & TESTMODES <*trace-level*> commands to produce a trace file ASIS*ASIS$TRACE$(*n*). Setting the trace level to 7 or higher usually works best. Use a full-screen editor to look at the file. Error messages and error codes usually appear after the calls to MSG_CALL_WITH_ID, which is the Messaging Integration Services call that the FLEX AMs issue. After looking at a few trace files, you can get a feel for them. The CALL SEC$USER$ is the Exec call that is used to map the Windows network user-id to the OS 2200 user-id. Error code 513 means that mapping failed. That is a common error. Check that the OS 2200 user-id record for this user has the proper network name in the network user-id field. Remember, the

network user-id in the OS 2200 security record must be entered in all uppercase characters.

- A UNISCOPE emulator has a tracing ability that may provide some diagnostic help. Normally, if the Kerberos or NT LAN Manager tickets cannot be created and sent to the OS 2200, these emulator traces are all that exists to diagnose the problem. Check the help system in the emulator you are using for their specific details on tracing.

  The emulator may return error messages after a failed $$OPEN attempt. These messages may contain Windows error codes and text. If no message is displayed after $$OPEN and the open fails to connect to the OS 2200, the path may not be configured correctly or the OS 2200 computer account may not have been entered correctly for that path in the emulator.

- Problems with 2200 Network Authentication configuration usually can be fixed with a reinstall of network authentication using Security Client. First select Delete Network Authentication from the Delete menu. Then select Install Network Authentication from the Install menu. If the reinstall works, the states of the authentication sentinel primary and alternative servers should show "available" on the Current Network Authentication screen (select Display Network Authentication from the Display menu).

  If the reinstall does not work, run with the Security Client trace option on and report the problem to Unisys support.

4.4. Hardware Troubleshooting

If you cannot resolve the problem through diagnostics and error messages, reboot the system by pushing the hard reset button on the slot appliance (Figure 4–1). You must reinstall network authentication using Security Client using the Install Network Authentication command in the Install menu.

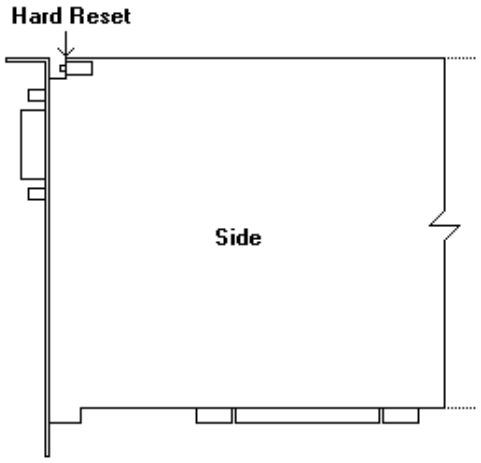

Figure 4–1. Location of Hard Reset Button

If the problem is still unresolved or recurs:

1. Power off the PCI rack.
2. Unplug all the wires from the failing slot appliance.
3. Remove the failing slot appliance.
4. Issue a UCF.
5. Send the slot appliance back to Unisys.
6. Wait for a new slot appliance to arrive.

If an update is needed but no problems exist on the current slot appliance, a new slot appliance will be shipped to replace the current one.

Appendix A
TIP/Demand Examples

The following examples describe how network authentication works in a TIP/demand environment.

TIP/Demand Example 1

The following procedure shows how Kerberos or NTLM authentication works if the user accesses the OS 2200 server by way of the INFOConnect Accessory Manager, a 2200 emulation product.

Note: *Other 2200 emulators can be used if they support the Windows Security Support Provider Interface (SSPI) to the 2200.*

1. From the Windows workstation, the user supplies a user name and password and then logs on to the Windows 2000 domain.
2. To access the OS 2200 server, the user enters $$OPEN from the Accessory Manager to a predefined path configured to use Kerberos or NTLM protocol for authentication. At this step, no solicitation for a user-id or password is required.
3. The Accessory Manager uses the Windows SSPI for authentication on the client side. Tokens generated by the SSPI are passed back and forth through the OS 2200 server to Authentication Sentinel for OS 2200. Authentication Sentinel for OS 2200 software uses the SSPI to perform server side authentication of the OS 2200 server.
4. Once the user on the OS 2200 server is authenticated, the principal name is obtained from the session ticket. If the principal name maps to a OS 2200 user-id, the user is deemed authentic for OS 2200 access.
5. Once the initial authentication is passed, the user may be solicited for additional information such as an account number, project-id, or clearance level if required by local OS 2200 authorization.

TIP/Demand Example 2

The following procedure shows how network user-id/password authentication works if the user accesses the OS 2200 server by way of a UTS terminal or an OS 2200 emulation product.

1. From the Windows workstation, the user supplies a user-id and password and then logs on to the Windows 2000 domain.
2. To access the OS 2200 server, the user enters $$OPEN from the Accessory Manager to a predefined path configured to use normal user-id/password

authentication. At this step, there is the normal solicitation for a user-id and password.

3. The *domainname\username/password* is entered by the user. The entered credentials can be the same credentials entered in step 1 or they can be another set of credentials.
4. The credentials are authenticated against the Windows Security Domain using Authentication Sentinel for OS 2200 software and the AM for user-id/password authentication on the OS 2200.
5. If the entered credentials are authentic, they are mapped to an OS 2200 user-id.
6. Once the initial authentication is passed, the user may be solicited for additional information such as an account number, project-id, or clearance level if required by local 2200 authorization.

Appendix B
Related Documents

***ClearPath Enterprise Servers Communications Application Program Interface User's Guide* (7851 5749)**

This guide explains how to develop application programs that use the services of the Communications Application Program Interface. It provides basic concepts necessary for designing applications to use the Communications Application Program Interface, and it contains detailed explanations of the Communications Application Program Interface TCP and UDP function calls.

***ClearPath Enterprise Servers Communications Interface for Transaction Applications Configuration and Operations Guide* (7862 6470)**

Communications Interface for Transaction Applications provides an interface for remote devices to access OS 2200 TIP applications using TCP/IP protocols. Communications Interface for Transaction Applications does not support any other transport or network protocols. The remote devices may be other OS 2200 systems, personal computers, or other systems.

***ClearPath Enterprise Servers Communications Platform Configuration and Operations Guide* (7844 8438)**

This guide provides task-oriented procedures and reference information for those responsible for configuring and operating the Communications Platform. It provides an overview of the product, identifies concepts/procedures for configuration and operation tasks, and identifies troubleshooting procedures

***ClearPath Enterprise Servers Messaging Integration Servers for ClearPath OS 2200 Help* (7851 5558)**

The NT Service Integration Assistant documents a message based service interface between a 2200 program and a Windows NT program. The Assistant is a Windows Help implementation.

***ClearPath Enterprise Servers User Authentication Administration Guide* (7850 4586)**

The User Authentication product allows implementation of stronger types of authentication for demand and TIP system access without local code.

ClearPath Enterprise Servers Security Administration for ClearPath OS 2200 Help (7862 1760)

This help system describes how to perform OS 2200 security operations such as signing on, changing passwords, and protecting files. It also describes how to configure, initialize, and maintain security using the Security-Admin product. It is provided as the Security Client help and also as a separate compiled HTML Help file, distributed on the ClearPath OS 2200 Product Information CD-ROM, for sites that do not use the Security-Admin product.

ClearPath Web Enablement Solutions Web Transaction Server for ClearPath OS 2200 Administration Guide (7850 4073)

This guide provides task-oriented information to help system administrators set up WebTS software. WebTS enables desktop users with Web browsers to access static Web pages and transaction programs in the OS 2200 environment of a ClearPath HMP IX server. You use WebTS administration software (WebTSA) running on a Windows 95 or Windows NT workstation to administer the WebTS server software.

47292016–000